This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (Canceled)

2. (Currently Amended) A system that detects the state of a computer network, comprising:

a plurality of distributed agents disposed in said computer network, each said distributed agent comprising:

data collection means for passively collecting, monitoring, and aggregating data representative of activities of respective nodes within said computer network;

means responsive to the data from the data collection means for analyzing said data to develop activity models representative of activities of said computer network in a normal state and activities of said computer network in an abnormal state as a result of intrusions, infections, scams and/or other suspicious activities in said computer network; and

means for comparing collected data to said activity models to determine whether said computer network is in said normal state or said abnormal state at different times and to dynamically update said activity models based on said collected data,

wherein said analyzing means performs a pattern analysis on the collected data to identify patterns in the collected data representative of suspicious activities and said comparing means compares the results of the pattern analysis of data collected by an agent to the results of pattern analysis of data collected by analyzing means of other agents to identify similar patterns of suspicious activity in different portions of the computer network.

3. (Canceled)

4. (Previously Presented) The system of claim 2, wherein said data collection means collects data representative of operation of said computer network, including respective nodes in said computer network, said data relating to communications, internal and external accesses,

code execution functions, and/or network resource conditions of respective nodes in said computer network.

5. (Previously Presented) The system of claim 2, wherein said activity models characterize conditions within said computer network including behaviors, events, and/or functions of respective nodes of said computer network, said behaviors representative of said normal state and one or more abnormal states representative of suspicious activity in said computer network.

6. (Previously Presented) The system of claim 2, further comprising means for characterizing the state of the computer network and identifying any potential threats based on said collected data.

7. (Previously Presented) The system of claim 6, wherein said characterizing means further recommends remedial repair and/or recovery strategies to isolate and/or neutralize the identified potential threats to the computer system.

8. (Previously Presented) The system of claim 2, wherein respective agents are connected by redundant communications connections.

9. (Previously Presented) The system of claim 2, wherein each agent is implemented in redundant memory and hardware that is adapted to be insulated from infected components of said computer network.

10. (Previously Presented) The system of claim 2, wherein the agents are disposed in a hierarchical structure whereby communications from bottom level agents to agents at higher levels in the hierarchy are limited.

11. (Previously Presented) The system of claim 2, further comprising means for predictively modeling the behavior of said computer network based on sequentially occurring behavior patterns in the data collected by said data collection means.

12. (Previously Presented) The system of claim 2, wherein said comparing means comprises means for pattern matching collected data with data in said activity models to determine a closest activity model based upon similarity of the data in each data model with the collected data.

13. (Previously Presented) The system of claim 2, wherein the collected data represents actions of a virus, system responses to actions of a virus, actions of a hacker, system responses to actions of a hacker, threats directed to discrete objects in said computer network, and/or potential triggers of a virus or threat to said computer network.

14. (Previously Presented) The system of claim 2, wherein said analyzing means for each agent filters and analyzes received data and dynamically redistributes the analyzed and filtered data to other agents associated with said each agent.

15. (Canceled)

16. (Previously Presented) The system of claim 2, wherein the comparing means compares names and email addresses in said collected data against known criminal, hoaxsters and/or aliases for known criminals and hoaxsters.

17. (Previously Presented) The system of claim 2, further comprising a trusted server that receives attack data from a plurality of agents identifying abnormal states indicative of a network attack, said trusted server gathering the attack data and sending warnings to selected nodes in said computer network.

18. (Currently Amended) A method of detecting the state of a computer network, comprising:

providing a plurality of distributed agents disposed in said computer network to passively collect, monitor, and aggregate data representative of activities of respective nodes within said computer network;

analyzing said data to develop activity models based on collected data and representative of activities of said network in a normal state and activities of said computer network in an abnormal state as a result of intrusions, infections, scams and/or other suspicious activities in said computer network, said data analysis including performing a pattern analysis on the collected data to identify patterns in the collected data representative of suspicious activities; and

comparing collected data to said activity models to determine whether said computer network is in said normal state or said abnormal state at different times and to dynamically update said activity models, said comparing including comparing the results of the pattern analysis of data collected by an agent to the results of pattern analysis of data collected by other agents to identify similar patterns of suspicious activity in different portions of the computer network.

19. (Previously Presented) The method of claim 18, wherein the agents report any suspicious activity that exceeds a suspicion threshold.

20. (Previously Presented) The method of claim 19, wherein the agents transmit said analyzed data in order to determine an origin of the suspicious activity in the computer network.

21. (Previously Presented) The method of claim 20, further comprising scanning said analyzed data for patterns and comparing said patterns to data representative of patterns of known threats to said computer network for identification of said suspicious activity.